 ISSN: 1411-3201

MASALAH KEAMANAN DAN PENGAMANAN SITUS WEB PEMERINTAH

Bayu Setiaji
STMIK AMIKOM Yogyakarta
bayusetiaji84@gmail.com

ABSTRAKSI

Belakangan ini banyak sekali aksi penyerangan terhadap situs web. Motif penyerangan tersebut seperti aksi protes terhadap hasil Pemilu, aksi protes terhadap kebijakan pemerintah atau hal yang lain, aksi balas dendam kepada pihak lain, bahkan hanya sekedar mencari sensasi. Keberhasilan aksi penyerangan tersebut didukung oleh banyak hal, salah satunya adalah dari sisi pengelola situs yang kurang memperhatikan hal – hal kecil yang berkaitan dengan masalah keamanan, sehingga membuka peluang untuk diserang.

Kata Kunci*: situs web, penyerangan, keamanan, pemerintah*

PENDAHULUAN

Ancaman yang sering dialami oleh pemilik dan pengembang website maupun blog adalah banyaknya berbagai jenis serangan di dunia maya. Dengan berbagai karakter dan motif penyerangan yang berbeda. Yang pasti membawa dampak negatif bagi website atau blog.

Semakin berkembangnya kehidupan di dunia maya, semakin beragam pula jenis-jenis serangan dan semakin meningkat pula kejahatannya. Untuk itu, keamanan di dunia internet ini harus ditingkatkan. Walaupun tidak ada yang paling aman di dunia maya! Kegiatan di dunia maya selalu tidak terlepas dari membuka alamat web satu ke alamat web yang lain. Atau melalui mesin pencarian. Dan sangat memungkinkan, alamat web yang kita kunjungi atau file-file yang kita download mengandung malware yang umumnya berupa spyware, adware, trojan, virus, worm, spam, dan exploit scripts.

KEAMANAN SITUS WEB PEMERINTAH

Ada banyak "lubang" yang bisa menjadi sasaran empuk bagi penyerang untuk melakukan aksi terhadap situs web sasaran. Rata – rata lubang tersebut berasal dari kelalaian pengelola situs web yang kurang memperhatikan masalah – masalah kecil.

1. Server Windows

Sebagian besar server web menggunakan sistem berbasis UNIX, dan sebagian kecil lainnya menggunakan Windows. Dalam hal ini tidak bisa dikatakan bahwa Windows adalah sistem yang lemah. Namun, sepanjang sejarah sistem Windows-lah yang paling banyak memegang rekor mendapatkan serangan.

Hal tersebut disebabkan karena eksploitasinya lebih menyenangkan dan lebih singkat. Ditambah lagi konfigurasi dan penerapan *policy* yang kurang tepat.

Hampir semua situs web pemerintah menggunakan server Windows yang tidak dikonfigurasi dengan baik. Ditambah lagi pengelolaan yang ditangani oleh pihak yang bukan ahlinya.

Sebenarnya pemerintah sudah menetapkan pedoman teknis untuk server web tetapi tidak semua instansi mematuhinya.

2. *Unsecure Password*

Password adalah satu hal yang sepertinya paling tidak dipedulikan keamanannya. Hampir semua situs pemerintah masih terdapat account dengan *password – password* yang mudah ditebak, seperti "123456", "admin", "administrator", "depkominfo", password menggunakan kode SKPD, dan masih banyak lagi.

Kurang pedulinya (atau kurang paham) pegawai instansi pemerintah terhadap keamanan password menjadi sesuatu yang sangat berbahaya. Mungkin saja suatu ketika ada *script kiddie* yang berhasil masuk ke area administrator dan mengacak – acak semua yang ada. Bisa jadi pekerjaan yang butuh waktu berbulan – bulan untuk menyelesaikannya, dapat hilang dalam waktu sesaat.

 ISSN: 1411-3201

3. *Web Mail*

Banyak situs web pemerintah yang masih menggunakan Squirrelmail, kendati sudah lama banyak isu keamanan yang muncul.

Salah satunya adalah tentang kemungkinan seorang *attacker* untuk menghapus seluruh isi *email* target secara diam – diam. Selain itu juga banyak *username* dan *password* yang sama.

4. File *backup* dan *SQL dump*

Banyak developer situs web yang lalai meninggalkan file SQL dump di direktori terbuka sehingga dapat di-*crawling* oleh mesin pencari, semisal Google. Hal tersebut memudahkan *attacker* untuk mencari informasi – informasi sensitif seperti *username* dan *password*.

Walaupun file – file tersebut sudah dihapus dari server, *attacker* masih bisa melihat isinya melalui *cache* yang dimiliki Google.

Bahkan parahnya lagi, ada developer yang menyimpan *account* FTP dan konfigurasi DNS-nya dalam file *.txt sehingga dapat ter-*crawling*.

Kejahatan di dunia maya dapat terjadi karena kesalahan pihak-pihak yang terlibat dalam pemakaian intenet. Kesalahan yang terjadi pada sisi pengembang diakibatkan oleh beberapa factor antara lain:

1. Kurangnya pengetahuan pengembang aplikasi website terhadap keamanan arsitektur software.
2. Perbedaan persepsi dan interpretasi antara pengembang dengan pemilik perusahaan.
3. Kesalahan syntax yang digunakan sehingga mengakibatkan celah keamanan sehingga memungkinkan terjadinya serangan.
4. Kesalahan pemilihan server dan hosting.
5. Kesalahan menggunakan method get / post dalam mengambil data client.
6. Kesalahan pengembang soft ware dalam menangani data penting yang diterima dari client tanpa dilakukan enkripsi.

Faktor penyebab serangan pada sisi client disebabkan oleh beberapa faktor antara lain:

1. Kurangnya pengetahuan tentang history dari browsing yang sudah dilakukan sehingga menjadi peluang bagi cracker.
2. Kurangnya kehati-hatian client dalam melakukan membuka situs tanpa melihat validitas dari alamat situs terlebih dahulu.
3. Kemudahan client dalam menerima dan menanggapi informasi yang diperoleh dari pihak ketiga tanpa dicek validitasnya.

Celah yang memungkinkan terjadinya serangan, diantaranya:

1. adanya lubang keamanan pada program. Sebuah program pasti terdapat eror atau lubang keamanan. Apabila lubang keamanan ini tidak segera ditutup, maka hal ini dapat dimanfaatkan untuk menyerang sistem atau program tersebut. Untuk itu, biasanya pengembang program selalu melakukan update atau perbaikan terhadap programnya.
2. serangan lewat email, berbagai macam serangan terhadap dunia maya, dapat dilakukan juga lewat email. Kode atau program dapat disisipkan lewat email yang masuk, yang dapat merusak sistem komputer atau melakukan tindak kejahatan lain di dunia maya.

LANGKAH PENGAMANAN

Ada banyak hal yang dapat dilakukan untuk melakukan pengamanan situs web dari aksi penyerangan, baik yang bersifat teknis maupun non-teknis.

1. Server Web yang Baik

Dari keterangan di atas, dapat disimpulkan bahwa sistem Windows mendapat rekor serangan paling tinggi, dikarenakan banyak faktor. Dalam hal ini sebaiknya developer web memilih server web yang lebih *reliable* dengan dukungan mesin yang sesuai.

2. Update

Developer mengusahakan untuk selalu melakukan *update* terbaru terhadap segala hal yang berada di server, misalnya sistem operasi yang digunakan, server web, server mail, server database, dan lain – lain.

Update tidak harus dilakukan dengan mengganti secara total, tetapi bisa dengan memasukkan *patch – patch* baru yang sudah disediakan oleh pihak penyedia.

3. Kerja Sama Web Master Profesional

Rata – rata situs pemerintah dikerjakan oleh developer yang ditunjuk dan bukan ahlinya. Hal tersebut boleh saja, tetapi untuk mengurangi resiko sebaiknya dibantu oleh *web master* profesional yang mengerti semua seluk – beluk tentang pengembangan situs web yang baik.

4. Mengetahui Cara Kerja *Attacker*

Langkah ini perlu dilakukan untuk memahami bagaimana para *attacker* bekerja sehingga pengelola situs web bisa melakukan langkah preventif untuk menanggulangi serangan semaksimal mungkin.

 ISSN: 1411-3201

Beberapa hal yang bisa dipelajari adalah *Remote File Inclusion (RFI)*[1]*, SQL Injection*[2]*,* dan *Cross Site Scripting (XSS)*[3].

5. Edukasi

Hal terpenting yang harus dilakukan adalah edukasi terhadap semua pihak yang berkepentingan dalam menggunakan situs web. Pengguna memegang peranan paling vital dalam masalah keamanan. Sebagus apapun sistem keamanannya, bila penggun melalaikannya maka tidak ada artinya apa – apa.

Dari beberapa kasus penyerangan, rata – rata disebabkan oleh kelalaian dari pihak pengguna maupun pengelola sendiri yang kurang peduli terhadap masalah keamanan.
Untuk itulah perlu ditanamkan pemahaman tentang masalah keamanan, mulai dari hal – hal kecil, semisal penggunaan password yang tidak mudah untuk ditebak, dan lain sebagainya.

Melalui Depkominfo sebenarnya pemerintah sudah mengeluarkan peraturan tentang **Pedoman Sistem Keamanan Web Server Untuk Instansi Pemerintah.**

Dalam peraturan tersebut semuanya tertulis secara detail tentang segala hal yang dapat digunakan sebagai acuan. Tips-tips untuk menjaga keamanan sebuah situs agar terhindar dari serangan dari sisi server :

1. Tidak perlu membuat script untuk mencari kesalahan login terletak pada username atau password. Karena jika penyerang telah mengetahui usernamenya, maka dia telah melewati celah keamanan pertama. Tinggal menebak passwordnya.
2. Hindari penggunaan username yang umum dan mudah ditebak seperti admin, administrator, dan seterusnya.
3. Cara pencegahan yang lain adalah dengan menolak penulisan script atau tag HTML, dengan resiko tampilan komentar menjadi datar tanpa aksesoris karena tag-tag HTML untuk melakukan variasi huruf (bold, italic, dan lain-lain) tidak dapat digunakan. Tetapi jika dibutuhkan, buat sendiri aturan dan penulisan tag, misalnya [:bold] untuk membuat huruf menjadi bold, dan seterusnya.
4. Gunakan pemrograman web secara terpisah antara satu modul dengan yang lainnya.
5. Jangan sepenuhnya mempercayakan validasi menggunakan HTML atau JavaScript, validasi kembali pada sisi server (bagaimanapun, validasi dari sisi client tetap diperlukan untuk keamanan dan kenyamanan pengguna awam).
6. Uji kembali parameter yang dikirimkan dan minimalkan kemungkinan terjadinya injection, gunakan function-function untuk membuang/mengubah karakter yang berbahaya dan tidak diperlukan. Contohnya karakter kutip yang sering digunakan dalam serangan SQL Injection ataupun karakter heksadesimal yang merepresentasikan karakter tertentu dalam beberapa serangan dengan metode Cross Site Scripting (XSS).
7. Pilih bahasa pemrograman yang sesuai. Usahakan menggunakan pemrograman server side scripting.
8. Enkripsi semua data penting dari client ke server ataupun sebaliknya.
9. Gunakan method post untuk mengambil data dan memproses request halaman.
10. Gunakan https untuk menangani form login dan SSL (Secure Socket Layer) untuk menangani transaksi e-commerce / perbankan.
11. Lakukan generate password secara berkala bagi admin yang menangani perawatan aplikasi web.
12. Buat DMZ (De Military Zone) jika aplikasi web yang dikelola merupakan aplikasi yang berharga.
13. Setting agar IP selalu ter *masking*. Dengan tujuan agar IP private menjadi IP public sehingga mempersulit penyerang untuk melakukan remote.
14. Back up data secara periodik sehingga jika terjadi serangan dan berhasil masuk ke server lebih mudah untuk mengembalikan ke keadaan normal.

KESIMPULAN

Dalam mengamankan situs khususnya situs pemerintah, harus ada petugas khusus untuk menjadi administrator web yang mempunyai pengetahuan tentang lubang

[1] Meng-*include*-kan file secara remote melalui *script* di server web

[2] Memanfaatkan kelemahan database dengan cara memasukkan string tertentu yang akan menjadi query

[3] Memasukkan script client-side ke halaman yang dilihat oleh user lain

 ISSN: 1411-3201

keamanan situs web seperti penggunaan Sistem Operasi untuk server, keamanan password, penggunaan web mail, SQL dump dll, yang biasanya celah dari itu menjadi jalan untuk penyerangan. sekaligus sang admin harus mengetahui tentang langkah - langkah pengamanan situs web seperti penggunaan web server yang baik, mengetahui cara kerja attacker dll.

Selain itu pihak pemerintah harus tanggap untuk segera memberikan penyuluhan kepada seluruh instansi pemerintahan akan pentingnya keamanan situs.

DAFTAR PUSTAKA

http://black-it.net/home/print-4da792cedb7eca78027800dd2912ed94.jsp, tanggal akses 26 April 2012 00:43

Dwi Santoso, Joko. 2011. *Manajemen Keamanan Jaringan Informasi Menggunakan IDS/TPS Strataguard*. Tesis. STMIK AMIKOM Yogyakarta